

**SEALED BY ORDER OF THE COURT****FILED**

Mar 05 2021

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE

**UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA**  
**SAN JOSE DIVISION**

6  
7  
8  
9  
10

FINJAN LLC,  
Plaintiff,  
v.  
SONICWALL, INC.,  
Defendant.

Case No. 17-cv-04467-BLF

**ORDER GRANTING IN PART AND  
DENYING IN PART DEFENDANT'S  
MOTION FOR PARTIAL SUMMARY  
JUDGMENT**

United States District Court  
Northern District of California

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

Plaintiff Finjan, Inc. (“Finjan”) brings this patent infringement lawsuit against Defendant SonicWall, Inc. (“SonicWall”), alleging infringement of eight<sup>1</sup> of Finjan’s patents: 6,154,844 (the “844 Patent”), 6,804,780 (the “780 Patent”), 7,613,926 (the “926 Patent”), 8,141,154 (the “154 Patent”), 8,677,494 (the “494 Patent”), 7,975,305 (the “305 Patent”), 8,225,408 (the “408 Patent”), and 6,965,968 (the “968 Patent”) (collectively, the “Asserted Patents”). Complaint (“Compl.”), ECF 1. Finjan alleges that it is entitled to enhanced damages pursuant to 35 U.S.C. § 284 because SonicWall has engaged in willful infringement of each of the Asserted Patents. *Id.* ¶¶ 72, 90, 106, 123, 140, 158, 170, 189, 206, 224.

Before the Court is SonicWall’s Motion for Partial Summary Judgment. Motion (“Mot.”), ECF 319-3; *see also* ECF 320 (redacted motion). On December 21, 2020, Finjan filed an opposition brief to the motion. Opposition Brief (“Opp.”), ECF 327-4; *see also* ECF 326 (redacted opposition brief). On December 31, 2020, SonicWall filed a reply brief. Reply Brief (“Reply”),

24  
25

<sup>1</sup> Finjan originally alleged infringement of ten patents. *See* Compl. The parties have since stipulated dismissal of Finjan’s claims of infringement of U.S. Patent Nos. 7,058,822 and 7,647,633. ECF 324.

ECF 335-3; *see also* ECF 336 (redacted reply brief). The Court heard oral arguments on January 14, 2021. ECF 341; *see also* Transcript (“Tr.”), ECF 354. The Court GRANTS IN PART and DENIES IN PART SonicWall’s Motion for Partial Summary Judgment.

## I. THE ACCUSED PRODUCTS

The infringement allegations subject to SonicWall’s motion for summary judgment relate to SonicWall’s cybersecurity products, to include (1) Gateways; (2) Email Security products (“ES products,” also referred to as “ESA”); (3) Capture Advanced Threat Protection (“Capture ATP”); (4) Gateways and Capture ATP; (5) ES products and Capture ATP; (6) Capture Client and Capture ATP; (7) Gateways and WAN Acceleration Appliance (WXA). Mot. at v.

SonicWall describes its products as follows: ES products receive emails that may contain attachments and perform numerous security-related tasks. In certain situations, the ES products may send email attachments to Capture ATP for analysis. SonicWall Senior Vice President and Chief Technology Officer John Gmuender Declaration (“Gmuender Decl.”), ECF 319-5 ¶ 8.

Gateways operate similarly to ES products, but [REDACTED] *Id.* at ¶ 5. When a Gateway sends packets to Capture ATP, [REDACTED] *Id.* at ¶ 12. [REDACTED] *Id.* at ¶¶ 5, 8.

Capture Client runs on an endpoint device. Just like Gateways and ES products, Capture Client can send files to Capture ATP for analysis. *Id.* at ¶ 10. Capture ATP analyzes files as they are received. As part of its analysis, Capture ATP [REDACTED] *Id.* at ¶¶ 12-13.

## II. LEGAL STANDARD

Federal Rule of Civil Procedure 56 governs motions for summary judgment. Summary judgment is appropriate if the evidence and all reasonable inferences in the light most favorable to the nonmoving party “show that there is no genuine issue as to any material fact and that the

moving party is entitled to a judgment as a matter of law.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). The current version of Rule 56 authorizes a court to grant “partial summary judgment” to dispose of less than the entire case and even just portions of a claim or defense. *See* Fed. R. Civ. P. advisory committee’s note, 2010 amendments; *Ochoa v. McDonald’s Corp.*, 133 F. Supp. 3d 1228, 1232 (N.D. Cal. 2015). As such, a court can, “when warranted, selectively fillet a claim or defense without dismissing it entirely.” *Id.*

The moving party bears the burden of showing there is no material factual dispute, by “identifying for the court the portions of the materials on file that it believes demonstrate the absence of any genuine issue of material fact.” *T.W. Elec. Serv. Inc. v. Pac. Elec. Contractors Ass’n*, 809 F.2d 626, 630 (9th Cir. 1987). In judging evidence at the summary judgment stage, the Court “does not assess credibility or weigh the evidence, but simply determines whether there is a genuine factual issue for trial.” *House v. Bell*, 547 U.S. 518, 559–60 (2006). A fact is “material” if it “might affect the outcome of the suit under the governing law,” and a dispute as to a material fact is “genuine” if there is sufficient evidence for a reasonable trier of fact to decide in favor of the nonmoving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

In cases like this, where the nonmoving party will bear the burden of proof at trial on a dispositive issue (e.g., patent infringement), the nonmoving party must “go beyond the pleadings and by her own affidavits, or by the ‘depositions, answers to interrogatories, and admissions on file,’ designate ‘specific facts showing that there is a genuine issue for trial.’” *Celotex*, 477 U.S. at 324. For a court to find that a genuine dispute of material fact exists, “there must be enough doubt for a reasonable trier of fact to find for the [non-moving party].” *Corales v. Bennett*, 567 F.3d 554, 562 (9th Cir. 2009). In considering all motions for summary judgment, “[t]he evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in his favor.” *Anderson*, 477 U.S. at 255.

### III. DISCUSSION

SonicWall asks the Court to issue an Order finding that:

- SonicWall does not infringe claim 1 of Patent '154;
- The combination of SonicWall's Email Security products and Capture ATP cannot infringe the asserted claims of Patent '844, '494 and '926;
- SonicWall Gateways do not receive "Downloadables" and therefore cannot infringe the asserted claims 10 and 14 of Patent '494, claims 41 and 43 of Patent '844, and the asserted claim of Patent '780 Patent;
- SonicWall does not infringe the asserted claims Patents '305 and '408 based on a combination of separate, remote computers;
- SonicWall does not infringe the asserted claims of Patents '926 and '305;
- Finjan is not entitled to a royalty on SonicWall's Non-U.S. Sales; and
- Finjan is not entitled to damages prior to actual notice of infringement of Patents '926, '968, '844, and '780.

Mot. at viii. The Court considers each request in turn.

#### **A. Non-Infringement of the '154 Patent**

SonicWall first requests the Court find that the Accused Products do not infringe claim 1 of Patent '154. The '154 Patent is directed to a system and a method "for protecting a client computer from dynamically generated malicious content[.]" '154 Patent at Abstract. Conventional reactive antivirus applications perform file scans looking for a virus's signature against a list known virus signatures kept on a signature file and thus, cannot protect against first time viruses or if a user's signature file is out of date. '154 Patent at 1:25-31, *id.* at 2:32-37. Proactive anti-virus application, on the other hand, use "a methodology known as 'behavioral analysis' to analyze computer content for the presence of viruses." *Id.* at 1:56-58.

Dynamic virus generation occurs at runtime where dynamically generated HTML contains malicious JavaScript code. '154 Patent at 3:53-64. For example the JavaScript function `document.write()` is used to generate dynamic HTML at runtime. *Id.* at 3:53-57. Malicious code inserted in a `document.write()` function would not be caught prior to runtime because the

malicious code is not present in the content prior to runtime. *Id.* at 3:65-4:4. To this point, the '154 Patent concerns a “new behavioral analysis technology [that] affords protection against dynamically generated malicious code, in addition to conventional computer viruses that are statically generated.” *Id.* at 4:31-34.

The basic setup of the '154 Patent involves three components: (1) gateway computer including a content modifier, (2) client computer including a content processor, and (3) security computer including an inspector, a database of client security policies, and an input modifier. '154 Patent at 9:5-11. A preferred embodiment describes a gateway computer that receives content including a call to an original function and an input. *Id.* at 5:6-9. The gateway computer then substitutes the call to the original function with a corresponding call to a substitute function, which operates to send the input to a security computer for inspection. *Id.* at 5:10-15. The gateway computer transmits the “modified content from the gateway computer to the client computer, processing the modified content at the client computer.” *Id.* at 5:13-15. The client computer then transmits “the input to the security computer for inspection when the substitute function is invoked.” *Id.* at 5:15-17. The security computer first determines “whether it is safe for the client computer to invoke the original function with the input.” *Id.* at 5:17-19. The security computer then transmits “an indicator of whether it is safe for the client computer to invoke the original function with the input,” to the client computer. *Id.* at 5:19-22. The client computer invokes the original function “only if the indicator received from the security computer indicates that such invocation is safe.” *Id.* at 5:22-24.

Claim 1 of the '154 Patent provides:

A system for protecting a computer from dynamically generated malicious content, comprising:

a content processor (i) for processing content received over a network, the content including a call to a *first function*, and the call including an input, and (ii) for invoking a *second function* with the input, only if a security computer indicates that such invocation is safe;

a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked;

and a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

'154 patent, 17:32-44 (emphasis added).

The parties stipulated to the same constructions of “first function” and “second function” as the Court determined in *Finjan Inc. v. Cisco Systems, Inc.*, No. 17-cv-00072-BLF (“*Cisco*”). ECF 214; *see also Cisco*, Order Construing Claims in U.S. Patent Nos. 6,154,844; 6,804,780; 7,647,633; 8,141,154; 8,677,494, ECF 134 at 35. Relevant here, the Court in *Cisco* construed “first function / second function” as “substitute function / original function, which is different than the first function.” *Id.*

Both parties reference this Court’s prior Order in *Cisco* where the Court granted in part and denied in part Cisco’s motion for summary judgment on claim 1 of the ’154 Patent. *Cisco*, Order Granting in Part and Denying in Part Cisco’s Motion for Partial Summary Judgment of Noninfringement (“Cisco MSJ Order”), ECF 487 at 6-12. The Court granted summary judgment with respect to noninfringement of the asserted claims of the ’154 Patent by Cisco AMP Products. *Id.* at 11. In doing so, the Court agreed with Cisco that the accused AMP Products “[did] not substitute calls to functions into any content that it receives.” Cisco MSJ Order at 6. It also rejected Finjan’s remote creation infringement theory that a “hacker or some other process modifies the original content by inserting a substitute function in place of the original function.” *Id.* at 6-7. To the contrary, the Court found that the ’154 Patent’s own language required that the invention *itself* “replaces the ‘original’ function with a ‘substitute’ function – not an external factor such as a hacker.” Cisco MSJ Order at 7.

The Court denied summary judgment with respect to the infringement by the URL rewriting feature of the Cisco ESA Outbreak Filters. Cisco MSJ Order at 11-12. There, “Cisco

acknowledge[d] that Finjan identifie[d] some sort of substitution as to the URL rewriting feature – namely, the rewritten URL is a substitute for the original URL,” but nonetheless argued that “a URL is simply an address and thus, is neither a function nor a call to a function.” Cisco MSJ Order at 11 (internal quotation marks omitted). The Court rejected this argument, explaining that

the parties’ dispute concerning the manner in which Cisco’s URL rewriting feature utilizes URL functionality precludes summary judgment. Specifically, *the parties dispute whether a URL (or a portion thereof) can be a “function,” or a “call to function”* – with Cisco arguing that URLs are nothing more than addresses and Finjan responding that the processing of a URL can be a function.

*Id.* at 12 (emphasis added).

### 1. Literal Infringement

SonicWall argues that “none of the ’154 Accused Products<sup>2</sup> receives content including a call to a substitute function, as required by the claim and the agreed claim constructions.” Mot. at 2. It urges the Court to resolve as a matter of law two Finjan theories of literal infringement—remote creation of a first function and a URL rewriting—each of which parallels the issues raised and discussed in the Court’s *Cisco* summary judgment order. *See* Mot. at 3-5; *see also* Opp. at 1-2.

#### i. Remote Creation of a First Function

SonicWall argues that Finjan’s expert fails to “identify any call to a function that was substituted into the received content as part of the Accused Systems” and instead opines that “both the call to the ‘substitute function’ and the ‘original function’ *can exist within the content as originally created.*” Mot. at 3 (emphasis added). SonicWall argues that this interpretation “renders the word ‘substitute’ in the Court’s construction meaningless,” “ignores the Court’s construction[,] and fails as a matter of law, as it did in the *Cisco* case.” Mot. at 3-4. SonicWall also contends that

---

<sup>2</sup> The ’154 Accused Products are (1) Gateways, (2) Capture ATP, (3) Gateways with Capture ATP, (4) Capture Client with Capture ATP, (4) ES products, and (5) ES products with Capture ATP. *See* Mot. at v. Finjan’s ’154 infringement theories against the Gateways and Capture ATP alone are subject to SonicWall’s motion to strike. *See* ECF 299 at 7-9.



1 “nothing Finjan identifies as the ‘substitute function’ performs the security functionality of the  
2 claim – i.e., sending the ‘input’ to a security computer for inspection when invoked.” Mot. at 4.

3 “Finjan does not dispute that if the Court applies the claims as it did in *Cisco*, then the  
4 Court could grant summary judgment on that theory for the same reasons articulated in *Cisco*,  
5 namely the first function was substituted remotely by an ‘external factor.’” Opp. at 4. With respect  
6 to SonicWall’s second argument, Finjan asserts that “SonicWall’s argument is unclear, but the  
7 premise seems to be that the substitute function in the accused products does not ‘perform[] the  
8 security functionality of the claim.’” *Id.* According to Finjan, “that is not a requirement of the  
9 claim or the Court’s construction of the ‘first function.’” *Id.*

10 Nothing within the record persuades the Court to apply the claim language to Finjan’s  
11 remote creation theory differently than it did in *Cisco*. In *Cisco*, the Court explicitly rejected  
12 Finjan’s remote creation theory as “inconsistent with the patent’s specification and the Court’s  
13 Markman Order.” Cisco MSJ Order at 7. The Court explained that under this theory—where, as  
14 here, the “substitute function” is supplied by an external source outside the control of any accused  
15 product—was contrary to the plain language of the ’154 Patent:

16 “To enable the client computer to pass function inputs to the security  
17 computer and suspend processing of content pending replies from the  
18 security computer, *the present invention operates by replacing  
19 original function calls with substitute function calls within the  
20 content, at a gateway computer, prior to the content being received  
21 at the client computer.*”

22 *Id.* at 7 (quoting ’154 Patent at 4:55-60) (emphasis in original). Based on this claim language, the  
23 Court again concludes that “it is the ‘[i]nvention’ that replaces the ‘original’ function with a  
24 ‘substitute’ function – not an external factor such as a hacker.” MSJ Order at 7; *see also Finjan,*  
25 *Inc. v. Juniper Nets., Inc.*, 387 F.Supp.3d 1004 at 1010-11 (N.D. Cal. 2019) (“The claimed ‘first  
function’ then clearly involves the ‘substitute function,’ which sends the content’s input to the  
security computer for inspection once invoked. . . . the substitute function exists only after the



original content is modified at the gateway computer.”); *Finjan, Inc. v. Juniper Networks, Inc.*, No. C 17-05659 WHA, 2019 WL 3302717, at \*2 (N.D. Cal. July 23, 2019) (explaining that a “substitute function” supplied by an external system “ultimately amounts to the original content initially received by the claimed system” and not a “substitute” function). Because Finjan’s infringement theory fails to identify a substitute function consistent with the claim language, the Court need not reach SonicWall’s second argument regarding whether the identified substitute function preforms a security function.

## ii. ES Products: URL Rewriting Theory

Finjan’s remaining theory of infringement against the ’154 Patent involves the URL rewriting feature in SonicWall’s ES products. *See* Medvidovic Report (“Medvidovic Rep.”), ECF 319-6 ¶ 288 (outlining theory). SonicWall argues this theory is subject to summary judgment because “it is undisputed that it is the accused ES products that insert the rewritten URL into the received email.” Mot. at 5 (citing Medvidovic Rep. ¶ 293). In other words, according to SonicWall, its ES products do not receive content that includes a call to a “first function” as the claim requires because the rewritten URL does not exist until the ES product itself inserted it into a received email. Mot. at 5-6.

Finjan responds that its expert “Dr. [Nenad] Medvidovic explained that the ESA ‘has a content processor which processes-Internet-based content, e.g., with its email plugin chain,’ and that based on that processing the ‘ESA rewrites the URLs where the first function is the rewritten URLs,’ thus receiving substitute URL.” Opp. at 2 (internal citations omitted) (citing Medvidovic Rep. ¶¶ 292-293); *see also* Tr. 20:13-15 (“ESA takes the content that was received, passes it off to the plugin that does the rewrite, and receives the written URL back.”). Finjan further contends that a SonicWall witness confirmed this process when the witness stated that “Yes, the e-mail has a URL in it. When it gets rewritten, the original e-mail is removed, and the rewritten URL gets put in its place within the email.” *Id.* (citing King Transcript (“King Tr.”), ECF 392-8 at 66:1-4).

In *Cisco*, as here, Finjan alleged a URL rewriting infringement theory of the '154 Patent. Cisco MSJ Order at 12. But in *Cisco*, the “content processor” was a client device that received an email with a re-written URL (i.e., the first function). *Id.* The first function was substituted into the email by Cisco’s Outbreak Filters—which were entirely distinct from the client device. *Id.* Here, Finjan asserts that the “content processor” is the email plugin chain *within* the ES product. Medvidovic Rep. ¶¶ 292-293 (the ESA “has a content processor which processes-Internet based content, e.g., with its email plugin chain”); *see also* Tr. 21:16-24 (“the plugin is part of the ESA, part of the content processor”).

Claim 1 of the '154 Patent requires “a content processor (i) for processing content received over a network, the content including a call to a first function . . . .” Under this plain language, the content “received over a network” must include the “call to a first function” when it is received. Thus, the parties’ dispute can be distilled to whether the ES product receives content containing a first function *over a network* from the email plugin—despite the fact that the email plugin is part of the ES product.

There is no evidence before the Court that the ES products receive content over a network from the email plugin. The Medvidovic Report explains only that “ESA has a content processor which processes Internet-based content, e.g., with its email plugin chain,” “ESA processes emails and determines whether there are suspicious scripts or URLs in the content it receives,” and “ESA rewrites [] URLs.” Medvidovic Rep. ¶¶ 292-293. Nowhere does Finjan, let alone Dr. Medvidovic, offer any evidence that content leaves the ESA, traverses over a network to the ESA’s email plugin, and comes back to the ESA with a first function. *See* Tr. 21:1-8. Thus, as a matter of law the Court concludes that ESA does not satisfy the claim requirement of “processing content received over a network, the content including a call to a first function.”

## 2. DOE Theory

1           SonicWall argues that Finjan’s DOE theories of infringement against the ’154 Patent are  
 2           conclusory and that Dr. Medvidovic fails to provide a “purported equivalent for receiving content  
 3           including a call to a first function.” Mot. at 6 (citing Medvidovic Rep. ¶¶ 260, 278, 298, 319).  
 4           Finjan responds that Dr. Medvidovic’s analysis is “sufficient” and that “this is not a summary  
 5           judgment issue, rather it is a cross examination issue for trial.” Opp. at 3 (citing Medvidovic Rep.  
 6           ¶¶ 296-299).

7           Although infringement under the doctrine of equivalents is a question of fact, summary  
 8           judgment is proper “[w]here the evidence is such that no reasonable jury could determine two  
 9           elements to be equivalent.” *Warner–Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 39 n.  
 10          8 (1997). “A patentee must establish ‘equivalency on a limitation-by-limitation basis’ by  
 11          ‘particularized testimony and linking argument’ as to the insubstantiality of the differences  
 12          between the claimed invention and the accused device.” *Akzo Nobel Coatings, Inc. v. Dow*  
 13          *Chemical Co.*, 811 F.3d 1334, 1342 (Fed. Cir. 2016) (citation omitted).

14          Because Finjan has failed to establish “equivalency on a limitation-by-limitation basis”  
 15          summary judgment is proper here. Dr. Medvidovic’s discussion of DOE is broad and conclusory.  
 16          *Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1329 (Fed.Cir.2001) (“Broad  
 17          conclusory statements offered by Telemac’s expert are not evidence and are not sufficient to  
 18          establish a genuine issue of material fact.”). Dr. Medvidovic states that SonicWall’s ES products  
 19          “perform the same function the same way because they receive incoming content that include[s] a  
 20          call to a first function” and “achieve the same results because they modify content that they  
 21          receiving incoming content [sic] inspect the content using an engine, as antivirus, static analysis,  
 22          and dynamic analysis, for scanning, and proceed with the function call of the content is  
 23          determined safe [sic].” Even excusing that this general explanation is partially unintelligible,  
 24          nowhere does Dr. Medvidovic articulate an equivalent to the claim’s requirement of receiving  
 25

content that includes “a call to a first function.” This failure is particularly glaring given Finjan has not successfully identified a “first function” in its literal infringement theories.

\*\*\*

Finjan has failed to establish a material dispute of facts as to any of Finjan’s theories of infringement of the ’154 Patent. The Court GRANTS SonicWall’s Motion for Summary Judgment and finds that the Accused Products do not infringe claim 1 of Patent ’154.

**B. The Combination of SonicWall’s ES Products and Capture ATP Cannot Infringe The ’844, ’494, And ’926 Patents**

SonicWall moves for a finding that the combination of SonicWall’s ES products and Capture ATP cannot infringe the asserted claims of Patent ’844, ’494 and ’926. Mot. at 6-8. In support of this request, SonicWall contends that “Capture ATP was not available for use with any ES product until [after the relevant patents expired].” *Id.* at 7. It also argues that “the only sandbox accused of infringement in this case is the sandbox that is part of Capture ATP.” *Id.* at 8. Finjan responds that SonicWall’s argument errs because “[l]egally, commercial availability is not a requirement for infringement” and “[f]actually, the record is overwhelming that the combination of Capture ATP and SonicWall’s ESA products was at least made and used long before the ’844, ’494, and ’926 Patents expired in 2017.” Opp. at 4-5.

The Court credits Finjan’s legal argument that commercial availability is not the appropriate standard to consider. *See* 35 U.S.C. § 271(a) (“[W]hoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent.”); *Netlist v. Smart Storage Sys*, No. 13-5889, 2014 WL 1320325, at \*3 (N.D. Cal. Apr. 1, 2014) (35 U.S.C. § 271 “does not require that the infringing product be ‘commercially available.’”). And it is undisputed that each of the ’844, ’494, and ’926 Patents claims priority to U.S. Patent Application No. 08/790,097 (now U.S. Patent No. 6,167,520), which was filed on January 29, 1997. *See* ECF 1-2 (’844 Patent) at 19; ECF 1-5 (’926 Patent) at 27; ECF 1-8 (’494 Patent) at 3); *see also* Opp. at

1 4-6. Thus, the relevant patents expired on January 29, 2017. 35 U.S.C. § 154; *see* McDuff Report  
2 (“McDuff Rep.”), ECF 319-7 ¶ 95 (showing 1/29/2017 patent expiration date).

3 The outstanding question before the Court is whether there is a material dispute of fact as  
4 to whether SonicWall made and used Capture ATP in combination with ES products before  
5 January 29, 2017. SonicWall argues there is no dispute of fact that it did not make and use Capture  
6 ATP in combination with ES until February 2017, *see, e.g.*, Reply at 3, and points to the  
7 Gmuender Declaration in support. According to Gmuender, while the release of Capture ATP with  
8 select SonicWall *firewalls* occurred in August 2016, SonicWall’s *ES products* were unable to send  
9 content (e.g., email attachments) to Capture ATP until February 2017, when SonicWall Email  
10 Security 9.0 was released. Gmuender Decl. ¶ 7 (emphasis added). SonicWall also cites to two  
11 documents to corroborate Gmuender’s account. *See* SonicWall Email Security 9.0 Release Notes,  
12 February 2017, ECF 320-13 at 2-3 (describing Capture ATP as a new feature); SonicWall Email  
13 Security 9.0.1 Release Notes, April 2017, ECF 320-14 at 3-4 (“Capture Advanced Threat  
14 Protection (Capture ATP) is a cloud-based service that analyzes various types of content for  
15 malicious behavior, and *this function is being extended to Email Security beginning with version*  
16 *9.0.*” (emphasis added)); *see also* SonicWall SonicOS 6.2.6.0 Release Notes, August 2016  
17 (explaining that Capture ATP is “an add-on security service to the *firewall*” (emphasis added)).

18 Finjan points the Court to two pieces of evidence it believes create a meaningful dispute of  
19 fact. Opp. at 4-5. First, it identifies expert testimony from Dr. Eric Cole. Cole Transcript (“Cole  
20 Tr.”), ECF 327-14. Dr. Cole testified that the first date of infringement for “SonicWall’s  
21 Gateways, Capture ATP and Email Security combinations” was in 2012. *Id.* at 52:8-14. Finjan  
22 also cites a SonicWall document that “corroborate[s] that the combined system was made and sold  
23 long before 2017.” Opp. at 5. The document is titled “Capture ATP/Email Security Integration –  
24 Extending Advance Threat Protection to Email” and dated September 2016. Capture ATP/Email  
25 Security Integration Document, ECF 327-12. On a page titled “MRD: Integrate Capture ATP into

Email Security,” the document includes several bullet points including [REDACTED]  
[REDACTED]” and [REDACTED]  
[REDACTED] *Id.* at 00549277. Elsewhere, the  
document describes “ES/Capture Integration Challenges” and “ES/Capture: Additional Work.” *Id.*  
at 00549282, 00549290.

This evidence is neither “overwhelming” nor sufficient to raise a triable issue of fact. *See*  
Opp. at 5. Dr. Cole’s statement that “the first date of infringement would be the 2012 date” was in  
response to the question “So SonicWall’s Gateways, Capture ATP and Email Security  
combinations that you set forth above in paragraph 19 are not deemed to infringe [the ’844 patent]  
prior to 2012; correct?” Cole Tr. at 52:8-14. This testimony does not meaningfully speak to the  
alleged infringement of the *specific* combination of ES products and Capture ATP. *See* Reply at 4.  
And, even ignoring this flaw, Finjan fails to provide any factual basis for Dr. Cole’s opinion.  
*Novartis Corp. v. Ben Venue Labs., Inc.*, 271 F.3d 1043, 1051 (Fed. Cir. 2001) (“If all expert  
opinions on infringement ... were accepted without inquiry into their factual basis, summary  
judgment would disappear from patent litigation.”); *MShift, Inc. v. Dig. Insight Corp.*, 747 F.  
Supp. 2d 1147, 1165 (N.D. Cal. 2010) (“...unsupported conjecture or conclusory statements are  
insufficient to defeat summary judgment.”); *see* Cole Tr. at 57:25-56:3 (stating that he relied on  
SonicWall documents to form his opinion as to product release dates); Opp. at 5 (identifying only  
the above-referenced SonicWall document).

The September 2016 SonicWall document similarly fails to establish a meaningful dispute  
of fact. No reasonable person could infer from this document that SonicWall made and used  
Capture ATP and ES products in combination as of September 2016. First, there is uncontested  
evidence that MRD stands for Market Requirement Document, which generally instructs  
development teams how to build products. Gordineer Transcript (“Gordineer Tr.”), ECF 335-5 at

56:22-57:1 (“product market requirement documents -- so MRDs -- to tell development what to build.”). The purpose of an MRD is consistent with the document’s forward-looking language: [REDACTED] and [REDACTED] Capture ATP/Email Security Integration Document at 00549277 (emphasis added); *see also id.* at 00549282, 00549290 (document describing “ES/Capture Integration Challenges” and “ES/Capture: Additional Work”). Indeed, nothing in this document reflects that Capture ATP and ES products were in fact being made and used in tandem as of September 2016.

Because there is no meaningful dispute of fact that SonicWall did not make and use the combination of SonicWall’s Capture ATP and ES products until February 2017, the Court GRANTS SonicWall’s Motion for Summary Judgment and finds that the combination of SonicWall’s ES products and Capture ATP cannot infringe the asserted claims of Patent ’844, ’494 and ’926.

### **C. SonicWall Gateways do not receive Downloadables**

SonicWall requests that the Court make a finding that SonicWall Gateways do not receive “Downloadables” and therefore cannot infringe the asserted claims 10 and 14 of Patent ’494, claims 41 and 43 of Patent ’844, and claim 9 of Patent ’780 Patent. Mot. at 8-10. SonicWall argues that its accused Gateways never receive or obtain a “Downloadable,” as construed by the Court, and thus it does not infringe these claims. *Id.* at 8-9. Finjan responds that “SonicWall raises no claim construction disputes that are resolvable as a matter of law. Instead, SonicWall raises disputes of fact involving the application of the construed claims to the accused products.” Opp. at 6. Finjan also attacks the technical logic of SonicWall’s request, contending that “SonicWall’s argument that the way its gateways receive files over a network somehow does not constitute



1 ‘receiving’ is plainly incorrect. The gateways ‘receive’ program files exactly as every device on  
 2 the Internet does—in a sequence of network packets that contain the file’s bits.” *Id.*

3 Claim 10 of the ’494 Patent, claims 41 and 43 of the ’844 Patent, and claim 9 of the ’780  
 4 Patent each require the receiving or obtaining of a “Downloadable.” *See* ’494 Patent, cl. 10 (“a  
 5 receiver for receiving an incoming Downloadable”); ’844 Patent, cls. 41 and 43 (“[means for]  
 6 receiving a Downloadable”); ’780 Patent, cl. 9 (“a communications engine for obtaining a  
 7 Downloadable”); *see also* ’494 Patent, cl. 14 (“The system of claim 10 wherein the Downloadable  
 8 includes program script.”). The Court construed “Downloadable” as an “executable application  
 9 program, which is downloaded from a source computer and run on the destination computer.”  
 10 ECF 132 at 39; *see also* Cole Tr. at 69:17-25 (an “executable application program” is “a program  
 11 that can execute of run on a computer” such as a “piece of code that can actually execute, run, or  
 12 perform a function”).

13 SonicWall describes the relevant process as follows:

14 A file is transmitted over the Internet by (1) a sending device  
 15 splitting the file into multiple IP packets, each of which contains a  
 16 portion of the bits that comprise the file (e.g., an application  
 17 program), (2) the sending device then sends each packet over the  
 18 Internet (the packets can take different routes and arrive out-of-  
 19 order), and (3) the receiving device (the ultimate destination)  
 20 extracts the packet data and “reassembles” the file so it can be  
 executed. An IP packet includes an IP header (with source and  
 destination information) and a payload. The payload includes a  
 portion of the application program, but any given IP packet itself is  
 not executable because it does not contain the entirety of the file. To  
 be executable, the payloads of all of the IP packets must be extracted  
 and the file reassembled.

21 Mot. at 9 (citing Gmuender Decl.) (internal citations omitted); *see* Opp. at 6-8. It is undisputed  
 22 that SonicWall Gateways operate by “inspect[ing] the payload of each packet on a packet-by-  
 23 packet basis and then send[ing] each packet to its destination without extracting the data and  
 24 reassembling a file.” *Id.* at 9-10 (internal citations omitted); Opp. at 6 (“The [SonicWall] gateways  
 25

1 ‘receive’ program files exactly as every device on the Internet does—in a sequence of network  
2 packets that contain the file’s bits.”).

3 The parties’ disagreement centers on whether a device receives or obtains a Downloadable  
4 when it receives a sequence of packets of an executable file, but never re-assembles the packets  
5 into a final executable file format. Finjan argues that “it is also undisputed that every network  
6 device that receives a Downloadable does it in this very way: by receiving packets that contain the  
7 file.” Opp. at 8. SonicWall responds that as a matter of law “IP packets cannot meet the Court’s  
8 construction of a ‘Downloadable,’ which is ‘an executable application program, which is  
9 downloaded from a source computer and run on a destination computer.’” Reply at 4-5.

10 Where, as here, the application of a claim construction to undisputed facts is properly  
11 resolved at summary judgment. *MyMail, Ltd. v. AOL, Inc.*, 476 F.3d 1372, 1378 (Fed. Cir. 2007)  
12 (citing *Gen. Mills, Inc. v. Hunt-Wesson, Inc.*, 103 F.3d 978, 983 (Fed.Cir.1997) (“Where the  
13 parties do not dispute any relevant facts regarding the accused product ... but disagree over  
14 possible claim interpretations, the question of literal infringement collapses into claim  
15 construction and is amenable to summary judgment.”)). The Court’s construction of  
16 “Downloadable”—which the parties agreed upon—is an “*executable* application program, which  
17 is downloaded from a source computer and *run* on the destination computer.” ECF 132 at 9  
18 (emphasis added); *see also* Cole Tr., ECF 319-12 at 69:17-25 (“an executable application  
19 program” is “a piece of code that can actually execute, run, or perform a function on a system”),  
20 70:1-10 (“[the code] would have to be written in a certain way so that it can – can be executed”).  
21 This language plainly does not cover unassembled IP packets.

22 Finjan’s argument to the contrary relies on a logical fallacy. Although it is undisputed that  
23 network devices *transmit* files in a sequence of packets, *see* Mot. at 9-10, Opp. at 6, it does not  
24 necessarily follow that a network device that receives unassembled IP packets receives a  
25 Downloadable. And Finjan offers no evidence that the accused Gateways ever possess a

reassembled file or executable application. While Finjan emphasizes that transmitted IP packets “contain[]” Downloadables, *see generally* Opp. at 7, it offers no evidence that unassembled packets are an executable application program that can run on a destination computer, *see* Tr. at 48:4-5 (“You have not given me any evidence that this product, that the Gateway receives a Downloadable.”). Instead, the evidence before the Court suggests exactly the opposite. Gmuender Decl. ¶ 3 (“The receiving device extracts the packet data and reassembles the file so that it can be opened or executed”).

The Court GRANTS SonicWall’s Motion for Summary Judgment and finds that SonicWall Gateways do not receive “Downloadables” and therefore cannot infringe the asserted claims 10 and 14 of Patent ’494, claims 41 and 43 of Patent ’844, and claim 9 of Patent ’780 Patent.

#### **D. Non-Infringement of ’305, ’408 Patents based on same computer**

SonicWall requests that the Court find that it does not infringe the ’305 and ’408 Patents based on a combination of separate, remote computers. Mot. at 13-16. According to SonicWall, “[t]he asserted claims of both the ’408 and ’305 Patents require that all claimed steps (’408 Patent) and certain claimed components (’305) be performed by or located within the same computer.” *Id.* at 13. Because a combination of separate, remote computers cannot infringe the asserted claims as a matter of law, SonicWall argues that Finjan cannot properly accuse Capture ATP of infringing its patents *in combination with* Gateways and/or ES products. *Id.* Finjan responds that “[s]ummary judgment is not appropriate here because the claims of the ’408 and ’305 Patents are not limited to being ‘performed by or located within the same computer’ as SonicWall alleges.” Opp. at 9.

The ’305 Patent “provides a method and system for scanning content that includes mobile code, to produce a diagnostic analysis of potential exploits within the content.” ’305 Patent at 2:4-6. The relevant portion of asserted claims 5 and 6 state:

A security system for scanning content within a computer, comprising:

a network interface, *housed within a computer*, for receiving incoming content from the Internet on its destination to an Internet application running *on the computer*;

a database of parser and analyzer rules corresponding to computer exploits, stored *within the computer* . . .

'305 Patent, cl. 1 (emphasis added); *see id.* cl. 5 ("The security system of claim 1 further comprising . . ."), cl. 6 ("The system of claim 1 wherein the incoming content received from the Internet by said network interface is HTTP content . . ."). Finjan accuses two "combination" products of infringing these claims: Capture ATP (i) with the Gateways and (ii) with the ES products.

The '408 Patent is generally directed to a method of scanning content received by a computer and analyzing that content through the dynamic building of parse trees, in order to determine the existence of malicious code. '408 Patent at 1:19-20. The relevant portion of asserted claim 1 states:

A computer processor-based multi-lingual method for scanning incoming program code, comprising:

*receiving, by a computer*, an incoming stream of program code;

*determining, by the computer*, any specific one of a plurality of programming languages in which the incoming stream is written;

*instantiating, by the computer*, a scanner for the specific programming language . . . ;

*identifying, by the computer*, individual tokens within the incoming stream;

*dynamically building, by the computer* while said receiving receives the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules;

*dynamically detecting, by the computer* while said dynamically building builds the parse tree, combinations of nodes in the parse tree . . . ; and

1                                    *indicating, by the computer*, the presence of potential exploits

2                                    . . .

3                                    ‘408 Patent, cl. 1 (emphasis added); *see also id.* cl. 22 (“program code for causing a computer to

4                                    perform” each of the recited steps). Finjan accuses one “combination” product of infringing these

5                                    claims: Capture ATP with the Gateways.

6                                    With respect to each patent, the parties do not dispute the functioning of the Accused

7                                    Products; instead, they dispute whether the claim language requires that the relevant claims be

8                                    completed by one computer. *See* Mot at 13; Opp. at 9. In other words, with respect to the ’305

9                                    Patent, can network interface, Internet application, and database be within different computers?

10                                   And, with respect to the ’408 Patent, can the receiving, determining, instantiating, identifying,

11                                   dynamically building, dynamically detecting, and indicating be performed by different computers?

12                                   In support of its position, Finjan cites to various Federal Circuit authority it believes stands

13                                   for the proposition that, as a matter of law, the articles “a” and “the” have the connotation of “one

14                                   or more.” Opp. at 9 (citing *Convolve v. Compaq Comp. Corp.*, 812 F.3d 1313, 1321 (Fed. Cir.

15                                   2016), *Baldwin Graphic Sys. v. Siebert*, 512 F.3d 1338, 1342-43 (Fed. Cir. 2008), and *Symantec v.*

16                                   *Comput. Assocs. Int’l*, 522 F.3d 1279, 1291 (Fed. Cir. 2008)). SonicWall rebuts this interpretation

17                                   of the caselaw, contending that “the rule that ‘a’ can mean ‘one or more’ simply means that the

18                                   claims do not limit a claimed apparatus to having a single one of the claimed article. But to qualify

19                                   as a claimed article, an accused article must contain all specified elements in the claim.” Reply at

20                                   6 (internal citation omitted).

21                                   Caselaw favors SonicWall. In *Baldwin*, the Federal Circuit considered the district court’s

22                                   claim construction of a patent for packaged fabric rolls. The relevant claim of the patent stated:

23                                   32. A pre-packaged, pre-soaked cleaning system for use to

24                                   clean the cylinder of printing machines comprising in

25                                   combination:

(1) *a pre-soaked fabric roll* saturated to equilibrium with cleaning solvent disposed around a core, said fabric roll having a *sealed sleeve* which can be opened or removed from said fabric roll for use of said fabric roll, disposed therearound, and said system including

(2) means for locating said fabric roll adjacent to and operatively associated with a cylinder to be cleaned.

*Baldwin*, 512 F.3d at 1340 (internal citation omitted) (emphasis in original). The district court construed “a pre-soaked fabric roll” to mean “a *single* presoaked fabric roll.” *Id.* “In concluding that ‘a’ means ‘one’ in this context, the district court largely relied on the subsequent use of ‘said fabric roll’ as suggesting a singular fabric roll.” *Id.* Based on this construction, and because it was undisputed that defendant sold the accused fabric rolls in sets of three or between six and nine, but not individually, the district court granted defendant’s motion for summary judgment of non-infringement. *Id.* at 1341.

The Federal Circuit reversed, holding that the claim was not limited to cleaning system with a *single* pre-soaked fabric roll, explaining:

This description does not require a single pre-soaked fabric roll. Under the terms of this description, the plastic sleeve could be in intimate contact with multiple fabric rolls, like the plastic wrapping on a package of several hot dogs is in intimate contact with each of the hot dogs . . .

512 F.3d at 1343; *see also Convolve*, 812 F.3d at 1321 (“Thus, absent a clear intent in the claims themselves, the specification, or the prosecution history, we interpret ‘a processor’ as ‘one or more processors.’”). The Federal Circuit did not suggest that each claimed pre-soaked roll was not required to be saturated to equilibrium with cleaning solvent and have a sealed sleeve. *See id.* In other words, even though the court found that the claim language was broad enough to embrace multiple of a single claimed element, it was silent as to whether the use of “a” altered the intrinsic requirements of that claimed element. Extending *Baldwin* to the instant matter, the claim language of Patent ’305 covers a security system in which multiple computers each contain a network

1 interface, Internet application, and database and the claim language of Patent '408 covers a  
 2 method in which multiple computers *each* receive, determine, instantiate, identify, dynamically  
 3 build, dynamically detect, and indicate. *Baldwin* does not, however, stand for a proposition that  
 4 would permit multiple computers that each fulfill a different claim element. In short, *Baldwin*  
 5 provides Finjan no refuge.

6 The salience of this conclusion is underscored by *Unwired Planet L.L.C. v. Google, Inc.*,  
 7 660 F. App'x 974 (Fed. Cir. 2016). There, the Federal Circuit considered a patent specification that  
 8 “describe[d] particular methods and systems for the “delivery of graphical location information  
 9 regarding mobile resources.” *Id.* at 977 (internal citations omitted). The relevant claim stated in  
 10 part:

11 A method for use in providing location information regarding  
 12 mobile resources in a data enabled network, comprising the steps of:

13 providing *a server node* associated with at least one wireless  
 14 communication network assisted location finding system;  
 said server node being in selective communication with a  
 client node via the data enabled network;

15 receiving, at *the server node*, *network location information*  
 16 *regarding a mobile resource location*, said network location  
 17 information being obtained using said at least one network  
 18 assisted location finding system, wherein said network  
 location information is based on the location of said mobile  
 resource in relation to at least one fixed ground-based  
 wireless network structure having a known geographic  
 location;

19 accessing at *the server node*, geographical mapping  
 20 information for an area including said mobile resource  
 location;

21 . . .

22 *Id.* 977-78 (emphasis in original). “The district court construed the term ‘server node’ as ‘one or  
 23 more computers, each performing the receiving, accessing, processing, and transmitting services  
 24 specified in the claims.’ The court's construction thus required that *each computer* perform each  
 25



and every one of the claimed functions—receiving, accessing, processing, and transmitting.” *Id.* at 980 (internal citation omitted) (emphasis added). The Federal Circuit disagreed, finding that the district court “improperly imported a limitation into the claim” by requiring each computer to perform each specified function. *Id.* Instead, the Court found that separate computers could separately perform different claimed functions because doing so meant that a “single server node” performed all the required steps. *Id.* Here, neither Patent ’305 or ’408 recites a device analogous to the “server node” discussed in *Unwired Planet*. Patent ’305 recites a computer that includes various components while Patent ’408 recites a method in which a computer, much like the server node at issue in *Unwired Planet*, performs various functions.

For similar reasons, *Symantec* is inapt. In *Symantec*, the Federal Circuit considered “whether the term ‘computer system’ is properly limited to a single computer, or whether it covers a network of multiple computers.” 522 F.3d 1279, 1290 (Fed. Cir. 2008). The relevant claim stated:

1. In a system for transferring digital data for storage in a computer storage medium, a method of screening the data *as it is being transferred* and automatically inhibiting the storage of screened data containing at least one predefined sequence, comprising the steps of:

causing a quantity of digital data resident on a source storage medium to be transferred to a *computer system* having a *destination storage medium*

*Id.* at 1286 (emphasis in original). The Federal Circuit rejected the district court’s construction of the term “computer” and “computer system” to mean a “personal computer or workstation,” explaining that “nothing in the specification that would limit the meaning of the term ‘computer’ or ‘computer system’ to a single computer.” *Id.* at 1290; *see also 01 Communique Lab, Inc. v. LogMeIn, Inc.*, 687 F.3d 1292, 1297 (Fed. Cir. 2012) (holding “the location facility may be distributed among one or more locator server computers.”). Just as in *Unwired Planet*, where the

1 Federal Circuit concluded that multiple computers that compromised a single claimed server node  
2 could fulfill different claimed functions, the Federal Circuit in *Symantec* concluded that multiple  
3 computers that compromised a single computer *system* could fulfill different claim elements.

4 In light of the claim language, the parties' arguments, and the caselaw, the Court finds as a  
5 matter of law that claims 5 and 6 of the '408 Patent require the same computer that houses the  
6 network interface to also house the recited Internet application and database of parser and analyzer  
7 rules. The Court also finds as a matter of law that the recited steps in claims 1 and 22 of the '408  
8 Patent must be performed by the same computer. *See, e.g., FotoMedia Techs., LLC v. AOL, LLC*,  
9 CIV.A. 2:07-CV-255, 2009 WL 2175845, at \*6–7 (E.D. Tex. July 21, 2009) ("The Court does not  
10 rule that there cannot be more than one server, each capable of performing all of the recited steps,  
11 in the claimed system. However . . . the inventors did not claim a system that could distribute the  
12 steps of the claims at issue between various server computers.").

13 Because the parties do not dispute that (1) Capture ATP and Gateways and (2) Capture  
14 ATP and ES products involve separate, remote computers, and because the asserted claims of  
15 Patents '305 and '408 require that the relevant components and steps be within or performed by  
16 the same computer, the Court GRANTS SonicWall's Motion for Summary Judgment and finds  
17 that SonicWall does not infringe the asserted claims Patents '305 and '408 based on a combination  
18 of separate, remote computers.

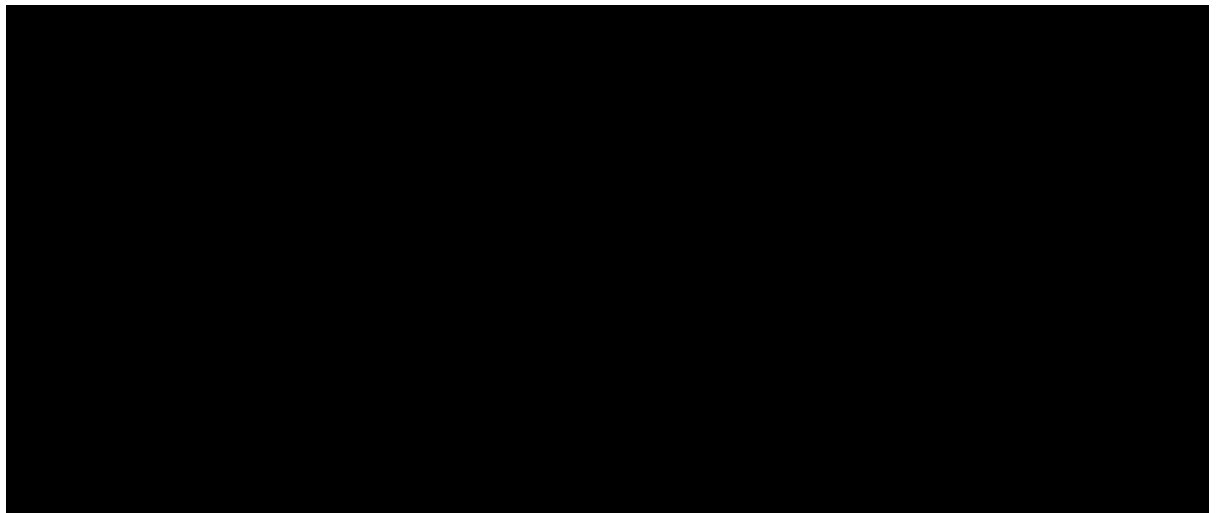
#### 19 **E. Non-Infringement of '926 Patent**

20 SonicWall asks the Court to find that Capture ATP does not infringe the asserted claims of  
21 Patent '926. Mot. at 16-19. In support of this request, SonicWall contends that Finjan has no proof  
22 that Capture ATP satisfies the patent's transmitter limitation, which requires that there is (i) a  
23 transmitter, (ii) that is coupled with the receiver that received the Downloadable, (iii) that  
24 transmits both an "incoming Downloadable" and a "representation of the retrieved Downloadable  
25

security profile data” (DSP), (iv) to a “destination computer,” (v) using a “transport protocol transmission.” Mot. at 16 (quoting ’926 Patent, cl. 22).

SonicWall contends that each of Finjan’s five theories regarding how Capture ATP satisfies that transmitter limitation fails as a matter of law as they are predicated on mischaracterized marketing and planning documents. Mot. at 16. At the motion hearing, SonicWall agreed to submit a chart identifying, for each of Finjan’s five theories regarding the ’926 Patent’s “Transmitter Limitation,” a *single* aspect of the transmitter limitation for which Finjan has failed to come forward with any evidence. *See* ECF 342. Finjan responds that SonicWall’s arguments are “plainly incorrect” and involve genuine disputes of fact. Opp. at 12.

**1. GRID Server/Threat Research Team as destination computer.** This theory is articulated by Dr. Michael Mitzenmacher, who states that “[REDACTED] Mitzenmacher Report (“Mitzenmacher Rep.”), ECF 327-16 ¶ 282. In support of this theory, Dr. Mitzenmacher includes the following diagram:



*Id.* Dr. Mitzenmacher also includes an excerpt of a SonicWall document that states:

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

*Id.* (emphasis in original).

In its supplementary chart, SonicWall highlights that this theory fails to account for the claim element “transmitting . . . a representation of the retrieved Downloadable security profile data.” ECF 342. SonicWall argues the theory is supported by a “[REDACTED] [REDACTED] [REDACTED]’ along with a statement in a second document that [REDACTED] [REDACTED].” Mot. at 16-17 (citing Mitzenmacher Rep. ¶ 282). Finjan responds that “[i]t is undisputed that Capture ATP does send the Downloadable to the GRID server: the documents say so.” Opp. at 12. It also argues, citing liberally to the Mitzenmacher Report, that “the record amply supports Finjan’s expert’s opinion that Capture ATP sends representations of security profile data to the destination computer.” *Id.* at 13.

The Court agrees with SonicWall that Finjan has failed to offer evidence of this claim element under the GRID server theory. Nothing in the chart Dr. Mitzenmacher relies on illustrates that a representation of a Downloadable security profile data—as opposed to a generic “malicious file”—is transmitted to the GRID server. *See* Mitzenmacher Rep. ¶ 282 (stating that representations of a Downloadable security profile include a score, verdict, confidence, or threat name); *Cf. PharmaStem Therapeutics, Inc. v. ViaCell, Inc.* 491 F.3d 1342, 1351-52 (Fed. Cir. 2007) (affirming district court’s judgment as a matter of law because marketing materials that do not speak to claim requirements are not substantial evidence of infringement). And rather than identifying additional evidence to support its theory, Finjan cites to paragraphs within the Mitzenmacher Report that rely on the same deficient diagram. *See, e.g.* Mitzenmacher Rep. ¶¶ 84-85, 282, 387-388.

██████████). In other words, undisputed evidence indicates that Capture ATP does not transmit a representation of a retrieved Downloadable security profile to the GRID server or the Threat Research Team. As such, this theory does not satisfy the transmitter limitation

27

1 evidence illustrate that “Capture ATP transmits files by reference to [the Sandbox database] via a  
2 file-hash pointer to the file’s location.” Opp. at 13.

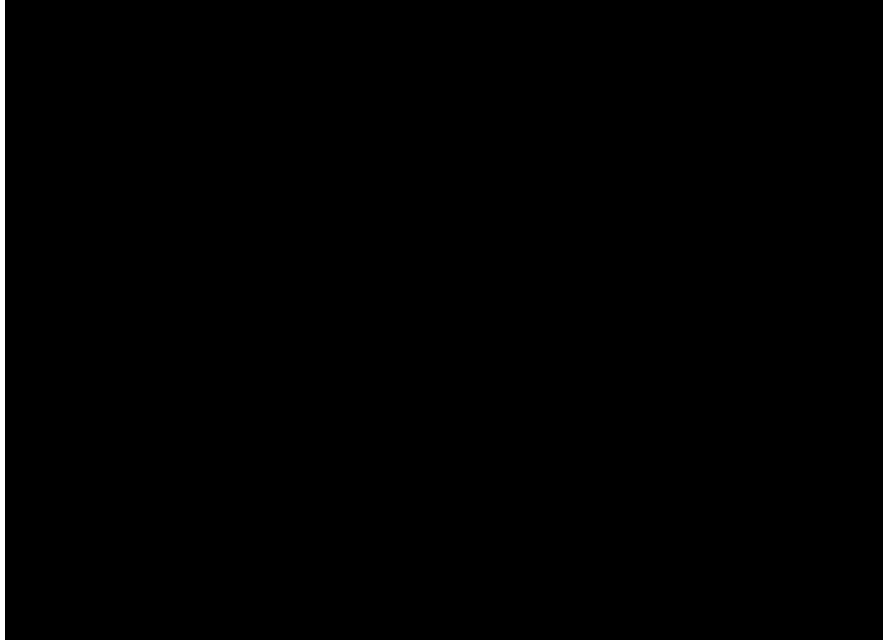
3 In its supplementary chart, SonicWall highlights that this theory fails to account for the  
4 claim element “transport protocol transmission.” ECF 342. According to SonicWall, “[w]hile  
5 Finjan’s expert notes that Capture ATP communicates with *other* SonicWall products (such as  
6 firewalls and client computers) by ‘using UFTP or HTTP protocols’, there is no evidence that such  
7 transmission protocols are used when components within Capture ATP (*e.g.*, the Sandbox  
8 Analyzer) communicate with other components *within* Capture ATP (*e.g.*, a database).” Mot. at  
9 17-18 (internal citations omitted) (emphasis in original). Finjan argues that it does provide this  
10 evidence, and cites to a SonicWall document that it claims “disclose[s] that Capture ATP  
11 communicates with third party applications using an API where various API commands are based  
12 on HTTP protocols.” Opp. at 14 (citing ECF 327-28 at 2575).

13 Under the Sandbox database theory, Capture ATP’s Sandbox Analyzer communicates with  
14 the Sandbox database via a transport protocol transmission. *See* Mitzenmacher Rep. ¶ 283  
15 (“Capture ATP has a transmitter in the Sandbox Analyzer for transmission of Sandbox file  
16 analysis . . . to the Sandbox database . . . sent over a network via protocol transmission (such as  
17 HTTP over TCP/IP, HTTPS, and UFTP”); ’926 Patent, cl. 22. The Court is hard-pressed to find  
18 evidence to this end. Finjan’s own expert confirms that the Sandbox analyzer and database are  
19 *internal* to Capture ATP. Medvidovic Report ¶ 68 (“Capture ATP includes databases and  
20 analyzers”). That Capture ATP uses transmission protocols when communicating with third party  
21 applications is irrelevant to whether the Sandbox Analyzer communicates with the Sandbox  
22 database via a transport protocol transmission. And while Finjan, over the silence of its expert,  
23 insists that “Capture ATP transmits files by reference to [the Sandbox database] via a file-hash  
24 pointer to the file’s location,” the record is devoid of evidence that a file-hash pointer to a file’s  
25 location involves a transmission protocol as required by the claim element. In particular, Finjan

1 offers no evidence that the downloadfile method transmits files as opposed to storing hashes of  
 2 files. And Dr. Mitzenmacher’s report includes no opinion that a skilled artisan would understand  
 3 storing a hash of a file has the same meaning as transmitting a file.

4 Because Finjan forwards no evidence that Capture ATP’s Sandbox Analyzer transmits a  
 5 representation of a retrieved Downloadable security profile to the Sandbox database via a transport  
 6 protocol transmission, this theory does not satisfy the transmitter limitation.

7 **3. Known file Database as destination computer.** This theory is articulated by Dr.  
 8 Mitzenmacher, who states that “Capture ATP transmits the downloadable to a known file database  
 9 (destination computer), along with a representation of DSP (such as a verdict and confidence) sent  
 10 over a network via protocol transmission (such as HTTP over TCP/IP, HTTPS, and UFTP).”  
 11 Mitzenmacher Rep. ¶ 286. In support of this theory, Dr. Mitzenmacher cites a single diagram titled  
 12 “Known file database integration”:



13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22 *Id.* (citing ECF 327-26 at 2539). Aside from the above chart, Finjan again invokes the  
 23 downloadfile method to argue that “Capture ATP transmits files by reference to [the known-file  
 24 database] via a file-hash pointer to the file’s location.” *See* Opp. at 13 (citing Mitzenmacher Rep. ¶  
 25 284; ECF 327-28 at 2586-2587).



In its supplementary chart, SonicWall highlights that this theory fails to account for the claim element “transport protocol transmission.” ECF 342. The Court agrees; nothing in the forward-looking internal document discusses a transport protocol transmission. *See* ECF 327-26 (“In order to improve the capture performance, we *would like to* create a known file database.”) (emphasis added). And, aside from the file-hash pointer theory that the Court has already rejected, neither the Mitzenmacher Report, nor Finjan’s opposition brief, identifies any other evidence detailing a transport protocol transmission. Accordingly, the Court concludes there is no factual dispute of fact that Capture ATP fails to satisfy the transport protocol transmission element of the transmitter limitation under this theory.

**4. Cloud Database as destination computer.** This theory is articulated by Dr. Mitzenmacher, who states that “Capture ATP transmits to a Cloud Database (aka Cloud db) (destination computer) in the cloud to store files along with a representation of their DSP (such as a verdict, score, confidence, threat name) sent over a network via protocol transmission (such as HTTP over TCP/IP, HTTPS, and UFTP).” Mitzenmacher Rep. ¶ 287. In support of this theory, Dr. Mitzenmacher excerpts a document that states [REDACTED]

[REDACTED]

[REDACTED]”

*Id.* (citing ECF 319-22 at 2558-2559). The document continues: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]” *Id.*

In its supplementary chart, SonicWall highlights that this theory fails to account for the claim element “transport protocol transmission.” ECF 342. The Court agrees; nothing in the cited document discusses a transport protocol transmission with any specificity. A document stating that the Sandbox Analyzer uploads a file to a cloud database is insufficient. And, aside from the file-

hash pointer theory that the Court has already rejected, neither the Mitzenmacher Report, nor Finjan’s opposition brief, identifies any other evidence detailing a transport protocol transmission. *See Opp.* at 13 (citing only to the Mitzenmacher Report); Mitzenmacher Rep. ¶¶ 287, 392 (excerpting same document). There is no factual dispute that Capture ATP fails to satisfy the transport protocol transmission claim element of the transmitter limitation under this theory.

**5. Capture Database as destination computer.** This theory is articulated by Dr.

Mitzenmacher, [REDACTED]

[REDACTED] ¶ 285. In support of this theory, he cites to a slideshow presentation slide with the title “Speaker Notes for Slide 4” that states

“ [REDACTED] ” *Id.* ¶ 285.

In its supplementary chart, SonicWall highlights that this theory fails to account for the claim element “transport protocol transmission.” ECF 342. Again, the Court agrees with SonicWall; nowhere in the identified slide is there a discussion of a transport transmission protocol, and, aside from the file-hash pointer theory the Court has already rejected, Finjan does not identify other evidence to illustrate that the claim element is satisfied. *See Opp.* at 13-15. There is no factual dispute that Capture ATP fails to satisfy the transport protocol transmission claim element of the transmitter limitation with respect to this theory.

**DOE.** SonicWall argues that “Finjan’s conclusory statements that the accused products perform the same function in the same way to achieve substantially the same results is insufficient to support a claim under DOE” with respect to the ’926 Patent. Mot. at 18-19 (internal citations omitted) (citing Mitzenmacher Rep. ¶¶ 288-291). Finjan responds that its theories are not conclusory and that SonicWall’s argument raises a factual dispute for the jury. *Opp.* at 15.

Because Finjan has failed to establish “equivalency on a limitation-by-limitation basis” summary judgment in favor of SonicWall is proper here. *Akzo Nobel Coatings*, 811 F.3d at 1342 (citation omitted). Dr. Mitzenmacher’s discussion of DOE is broad and conclusory. *Telemac*, 247 F.3d at 1329 (Fed.Cir.2001) (“Broad conclusory statements offered by Telemac’s expert are not evidence and are not sufficient to establish a genuine issue of material fact.”). For example, Dr. Mitzenmacher states that “Capture ATP performs the same function as this claim element because it transmits a Downloadable to a destination computer, and also transmits the Downloadable information with information generated from its Downloadable Security profile, including information corresponding to behaviors performed, like a score, verdict, or threat name to a destination computer.” Mitzenmacher Rep. ¶ 289. While Dr. Mitzenmacher emphasizes that “Capture ATP performs the same function” as the claim elements, he fails to articulate each limitation with any meaningful particularity—much less articulate how the differences between the two functions are insubstantial. See *Akzo Nobel Coatings*, 811 F.3d at 1343.

\*\*\*

The Court GRANTS SonicWall’s Motion for Summary Judgment and finds that Capture ATP does not infringe the asserted claims of Patent ’926.

#### **F. Non-Infringement of Patent ’305**

SonicWall asks the Court to find that it does not infringe the asserted claims of Patent ’305. Mot. at 19-20. Finjan asserts dependent claims 11 and 12 of the ’305 Patent, which rely on independent claim 1:

a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer

...

a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively *diverting*

incoming content from its *intended destination* to said rule-based content scanner; and

305 Patent, cl. 1; *see also id.*, cl. 11 (“The system of claim 1 wherein the destination Internet application is a web browser.”); cl. 12 (“The system of claim 1 wherein the destination Internet application is an e-mail client.”).

SonicWall argues that Finjan cannot prove that Capture ATP has “a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner” because content is never “diverted” from an “intended destination.” Mot. at 19. Finjan responds that SonicWall “mischaracterizes and ignores evidence that directly supports Finjan’s infringement theories” as to these claims. Opp. at 15. It also argues that “a fact dispute regarding the accused products selectively diverting incoming content from the intended destination precludes summary judgment as the parties disagree regarding how the claims read on the accused products.” Opp. at 15 (citing *Power Mosfet Techs., L.L.C. v. Siemens AG*, 378 F.3d 1396, 1406 (Fed. Cir. 2004) (The “determination as to whether the claims, properly construed, read on the accused device is a question of fact”).

Dr. Medvidovic asserts that “Capture ATP’s controller server or its Capture Engine” is the network traffic probe. Medvidovic Rep. ¶ 217. He further asserts the controller server or the Capture Engine causes incoming content to be selectively diverted from a web browser or email client on either Capture ATP’s virtual sandbox or an endpoint client computer to [REDACTED]. *Id.* ¶¶ 217-218. Dr. Medvidovic’s report can thus be distilled to two theories: one in which traffic is selectively diverted from the Capture ATP sandbox and one in which traffic is selectively diverted from the client endpoint. In both theories, the traffic is diverted to [REDACTED]

1           ***Selective diversion from virtual sandbox.*** Under Finjan’s first theory, files are diverted  
 2 from Capture ATP’s virtual sandbox [REDACTED]. SonicWall contends that this  
 3 theory “strains credulity” because “[t]he ‘intended destination’ is the destination to which content  
 4 (files) is sent *before* the security system intervenes and ‘selectively diverts’ it (via the network  
 5 traffic probe) to a scanner. Even accepting Finjan’s premise that Capture ATP is an ‘intended  
 6 destination,’ files analyzed in Capture ATP [REDACTED]  
 7 Mot. at 20 (citing Gmuender Decl. ¶ 12) (emphasis in original). Finjan responds by citing to  
 8 documents in the Medvidovic Report that “[REDACTED]  
 9 [REDACTED]  
 10 [REDACTED]  
 11 [REDACTED] Opp. at 17-18 (citing Medvidovic Rep. ¶¶ 217-218).

12           A review of the evidence cited by Dr. Medvidovic tells a different story. Finjan points to  
 13 various documents to support its theory. For example, Finjan cites to a document titled  
 14 “SonicSandbox high level design,” which Finjan contends “[REDACTED]  
 15 [REDACTED]” ECF 319-36 at 873020, 873022, along with a document titled  
 16 “Automated Real-Time Breach Detection and Prevention Technology,” SonicWall-  
 17 Finjan\_00639853 at 9869. Neither the Medvidovic Report nor the opposition brief explains how  
 18 these documents support Finjan’s infringement theory; indeed, the documents do not reference a  
 19 selective diversion from the sandbox virtual machine to the Capture ATP pre-filters.

20           The only potentially relevant document before the Court is titled “SonicSandbox 2.2:  
 21 Functional Specification” and states “[REDACTED]  
 22 [REDACTED] ECF 319-22 at 2559. Finjan claims that this  
 23 document [REDACTED]” Opp. at 17.  
 24 The Court disagrees. This document fails to give rise to an inference that files are selectively  
 25 diverted from [REDACTED]. Instead, in the context of Finjan’s

theory, it suggests just the opposite—that [REDACTED]

[REDACTED]. This inference is consistent with Gmuender’s declaration:

[REDACTED]

Gmuender Decl. ¶¶ 12-13.

Finjan fails to provide the evidence required under this theory that files are diverted from Capture ATP’s virtual sandbox to [REDACTED]

***Selective diversion from client endpoint.*** Under Finjan’s second theory, files are diverted from a client endpoint to [REDACTED].<sup>3</sup> SonicWall contends that “undisputed record evidence shows that [REDACTED]

[REDACTED] Mot. at 19 (citing Zhu Tr. at 208:19-209:18) (emphasis in original). Finjan responds by citing to

documents in the Medvidovic Report that [REDACTED]

[REDACTED] Opp. at 17 (citing Medvidovic Rep. ¶¶ 217-218). The cited documents refer to Capture ATP’s Block Until Verdict (“BUV”) feature. SonicWall replies that these marketing documents “offer[] no evidence to show *how* the BUV feature works” and that uncontested evidence shows that “[REDACTED]

<sup>3</sup> This theory is subject to SonicWall’s motion to strike. *See* ECF 299 at 1-3.

As an initial matter, the Court agrees with SonicWall that the Medvidovic Report does not explain with any meaningful particularity how Capture ATP's BUV operates. *See* Medvidovic Rep. ¶ 217 ("Capture ATP can block the content until verdict as well as perform zero day detection and blocking."); *cf. Novartis*, 271 F.3d at 1051 ("If all expert opinions on infringement ... were accepted without inquiry into their factual basis, summary judgment would disappear from patent litigation."). SonicWall, however, offers undisputed evidence that [REDACTED]

Even accepting Dr. Medvidovic’s vague characterization of BUV, Finjan’s infringement theory fails as a matter of law. The ’305 Patent claim language plainly requires that there be a selective diversion of incoming content from its intended destination (i.e., the client endpoint) to a rule-based content scanner (i.e., [REDACTED]). *See* ’305 Patent, cl. 1 (“a network traffic probe . . . for selectively diverting incoming content from its intended destination to said rule-based content scanner”). In other words, selective diversion must occur *before* content is analyzed by a rule-based scanner. *See* Tr. at 74:21-24 (“I read the patent as saying selective diversion is before the analysis.”), 76:6-10 (“So that’s exactly my point here is that this is selective diversion for the purpose of analysis, is how I’m reading the claim, as opposed to selective diversion which would then be to the garbage can, obviously.”).

Medvidovic Rep. ¶ 217 (emphasis



1 added); *see also* Opp. at 17 [REDACTED]  
2 [REDACTED]  
3 [REDACTED]” (emphasis added)). Finjan confirmed this timeline during the motion hearing. Tr.  
4 at 73:14-18 (“you intended that particular file to end up at the client's computer. But instead, when  
5 you came in, is you ran Capture ATP and you analyzed the particular file or particular content, and  
6 you made the selective diversion.”), 74:17-18 (“It's selective because unless you got the positive  
7 verdict back, you are not going to send it over.”). Finjan’s theory is inconsistent as a matter of law  
8 with the claim language.

9 \*\*\*

10 Because there is no genuine dispute of fact that Capture ATP does not selectively divert  
11 files, as the claims require, to [REDACTED], as Finjan theorizes, the Court  
12 GRANTS SonicWall’s Motion for Summary Judgment and finds that it does not infringe the  
13 asserted claims of Patent ’305.

## 14 **G. Damages**

### 15 **1. Foreign Sales**

16 SonicWall moves for a finding that Finjan is not entitled to a royalty on SonicWall’s  
17 foreign sales. Mot. at 20-22. SonicWall argues that Finjan’s damages expert Dr. DeForest McDuff  
18 improperly opines that a reasonable royalty is calculated “based on SonicWall *worldwide* sales.”  
19 Mot. at 21 (quoting McDuff Report (“McDuff Rep.”), ECF 319-7 ¶ 8) (emphasis added). Finjan  
20 responds that “evidence confirms SonicWall’s business with non-U.S. entities (e.g., the revenue,  
21 unit sales, and scans addressed by the motion) directly arises from acts of domestic infringement.  
22 In such cases, customers’ overseas locations are ‘irrelevant’ to liability.” Opp. at 19 (quoting *R.R.*  
23 *Dynamics, Inc. v. A. Stucki Co.*, 727 F.2d 1506, 1519 (Fed. Cir. 1984) (“Whether [infringing]  
24 carsets were sold in the U.S. or elsewhere is irrelevant[.]”)).  
25

The Court first considers the McDuff Report. Dr. McDuff explains that he calculated Finjan's reasonable royalties by looking to "SonicWall worldwide sales (for which infringement of the Patents-in-Suit occurs in the United States)." ECF 319-7 ¶ 8. Dr. McDuff continues:

I further understand that sales of Accused Products that occur outside of the U.S. can infringe the claims of U.S. patents if, for example, such foreign sales are tied to U.S. infringing activity, *e.g.* manufacturing or testing of Accused Products occurs within the U.S. In this case, I understand that SonicWall's foreign sales outside of the U.S. are accused of being implicated by SonicWall's infringement of Finjan's U.S. patents, based upon: (a) the presence of SonicWall Capture ATP and GAV/IPS servers within the U.S., (b) the majority of viruses originate in the United States and signatures are created from these, benefitting SonicWall's entire ecosystem, and (c) the email source code depository is stored in [California]. Accordingly, I have calculated the royalty base for U.S. sales, sales outside the U.S., and combined global sales in the event all worldwide sales are implicated by SonicWall's infringement.

*Id.* ¶ 92. The parties do not dispute the evidence on which Dr. McDuff relies; instead, they dispute whether this evidence establishes that Finjan may claim royalties for worldwide sales. *See Reply* at 11-12.

"It is axiomatic that U.S. patent law does not operate extraterritorially to prohibit infringement abroad." *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348, 1371 (Fed. Cir. 2013) (citation omitted); *see also Microsoft Corp. v. AT & T Corp.*, 550 U.S. 437, 441 (2007) ("It is the general rule under United States patent law that no infringement occurs when a patented product is made and sold in another country."); *cf. Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949) (courts presume that federal statutes "apply only within the territorial jurisdiction of the United States."). 35 U.S.C. § 271, the statute under which Finjan seeks damages, states in relevant part that

whoever without authority makes, uses, offers to sell, or sells any patented invention, *within the United States* or imports into the United States any patented invention during the term of the patent therefor, infringes the patent.

(emphasis added). Despite this overarching rule, Finjan contends that Supreme Court and Federal Circuit law “confirm[] that overseas revenues, when they arise from domestic infringement, are to be considered for damages.” Opp. at 20 (citing *WesternGeco LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129 (2018), *R.R. Dynamics*, 727 F.2d 1506).

Finjan’s argument overreads the caselaw. In *WesternGeco*, the Court explained that 35 U.S.C. § 271(a) – which Finjan’s infringement claim is based upon – “covers most infringements that occur ‘within the United States,’” whereas § 271(f)(2) – the subsection it was addressing – “expands the definition of infringement to include supplying from the United States a patented invention’s components.” 138 S. Ct. at 2134. The Supreme Court ruled that the presumption against extraterritoriality did not apply to a claim for lost profits under § 271(f)(2), but declined to extend its holding beyond that specific subsection. *Id.* at 2136-39. And in *R.R. Dynamics*, the plaintiff admitted to “making” the accused product in the United States. 727 F.2d at 1519.

Finjan cannot recover worldwide royalties under § 271(a) based solely on the evidence on which Dr. McDuff relies. “The use of a claimed system under section 271(a) is the place at which the system as a whole is put into service, *i.e.*, the place where control of the system is exercised and beneficial use of the system obtained.” *NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282, 1317 (Fed. Cir. 2005); *cf. id.* at 1318 (“Under section 271(a) . . . [i]t is well established that a patent for a method or process is not infringed unless all steps or stages of the claimed process are utilized.” (internal quotation marks omitted)). Courts have interpreted the word “use” broadly; the Supreme Court explained in *Bauer & Cie v. O'Donnell* that “use,” as used in a predecessor to title 35, is a “comprehensive term and embraces within its meaning *the right to put into service any given invention.*” 229 U.S. 1, 10-11 (1913) (emphasis added); *see also NTP*, 418 F.3d at 1316-1317 (discussing the meaning of “uses ... within the United States”). Moreover, “direct infringement by ‘use’ of a system claim requires a party ... to use each and every ... element of a claimed [system].” *Centillion Data Sys. v. Qwest Commc’ns Int’l, Inc.*, 631 F.3d 1279, 1284 (Fed.

1 Cir. 2011) (alterations and ellipses in original). To “use” a system, “a party must put the invention  
2 into service, *i.e.*, control the system as a whole and obtain benefit from it.” *Id.*

3 Caselaw clearly precludes Dr. McDuff from relying on “the presence of SonicWall  
4 Capture ATP and GAV/IPS servers within the U.S.” and the fact that “the majority of viruses  
5 originate in the United States and signatures are created from these, benefitting SonicWall’s entire  
6 ecosystem” to establish worldwide royalties. ECF 319-7 ¶ 92. When a foreign customer submits a  
7 file to Capture ATP, it is the customer—not SonicWall—that uses the claimed system because  
8 “direct infringement by ‘use’ of a system claim requires a party ... to use each and every ...  
9 element of a claimed system.” *Centellion*, 631 F.3d at 1285. And this customer’s use of Capture  
10 ATP occurs abroad because the customer’s location is “the place at which the system as a whole  
11 is put into service, *i.e.*, the place where control of the system is exercised and beneficial use of the  
12 system obtained.” *NTP*, 418 F.3d at 1317. This is true even if part of the system, such as the  
13 Capture ATP server, is located within the U.S. *See, e.g., CNET Networks, Inc. v. Etilize, Inc.*, 528  
14 F. Supp. 2d 985, 991 (N.D. Cal. 2007) (where “the situs of use of the system as a whole ... is  
15 Pakistan, not the United States,” there is no domestic infringement). By similar logic, it is  
16 irrelevant that Capture ATP [REDACTED]

17 [REDACTED] Opp. at 19. Finjan stresses that “SonicWall relies on the key signature  
18 database deriving from [the use of Capture ATP] to provide significant value for its customers  
19 worldwide—both domestic and overseas.” *Id.* at 20. But this is not the law, and Finjan’s logic  
20 would swallow up 35 U.S.C. § 271(a) in its entirety.

21 Nor can Dr. McDuff rely on evidence that SonicWall’s “email source code depository is  
22 stored in [California].” ECF 319-7 ¶ 92. The Court agrees with Finjan that several of the claims  
23 at issue—Patent ’844, claim 41 and Patent ’408, claim 22—are computer-readable medium  
24 (CRM) claims. These claims are infringed whenever patented code is made, copied, or stored.  
25 *E.g., Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1204–05 (Fed. Cir. 2010)

(describing how a CRM claim requires only that the code be “written”). But the fact that SonicWall maintains a source code depository in the United States is insufficient to establish domestic infringement. To this end, the Supreme Court has made clear that liability does not “extend to computers made in another country when loaded with [] software copied abroad *from a master disk or electronic transmission* dispatched by [defendant] from the United States.” *Microsoft*, 550 U.S. at 442 (emphasis added). Extending the Supreme Court’s logic to the instant case, Finjan must provide evidence that SonicWall makes domestic copies of ESA code and sells those specific copies overseas. It has failed to do so. *See Opp.* at 20-21 (relying solely on the location of SonicWall’s code depository).

Because the evidence on which McDuff relies cannot support Finjan’s claim for worldwide royalties as a matter of law, the Court GRANTS SonicWall’s Motion for Summary Judgment and finds that Finjan is not entitled to a royalty on SonicWall’s foreign sales.

## 2. Notice of Infringement

SonicWall moves for a finding that Finjan is not entitled to damages prior to actual notice of infringement of Patents ’926, ’968, ’844, and ’780. *Mot.* at 22-25. SonicWall argues that even if Finjan’s discussions with Dell, SonicWall’s predecessor, could be imputed to it, Finjan nonetheless failed to provide actual notice of infringement by the accused products. *Mot.* at 22-23. Finjan responds that the record clearly establishes that SonicWall was on notice since mid-2014. *Opp.* at 21-22 (citing *SRI Int’l, Inc. v. Advanced Tech. Labs., Inc.*, 127 F.3d 1462, 1470 (Fed. Cir. 1997) (“The requirement of actual notice under § 287(a) is designed to assure that the recipient knew of the adverse patent during the period in which liability accrues[.]”)). According to Finjan, “SonicWall’s complaints that the notice back then did not reflect the specific infringement theories to be tried years later or name every currently accused product *in haec verba* are off point.” *Opp.* at 22.

1 Although Finjan vigorously insists that SonicWall attempts to impose a heightened notice  
2 requirement, *see* Opp. at 22, the Court finds to the contrary. The law here is straightforward and  
3 Finjan shoulders the “burden of pleading and proving at trial that [it] complied with the statutory  
4 requirements” of 35 U.S.C. § 287(a). *Maxwell v. J. Baker, Inc.*, 86 F.3d 1098, 1111 (Fed. Cir.  
5 1996). Finjan must prove that for each asserted patent it communicated a specific charge of  
6 infringement by a specific accused product. *Amsted Indus. Inc. v. Buckeye Steel Castings Co.*, 24  
7 F.3d 178, 187 (Fed. Cir. 1994). When a plaintiff meets “the threshold specificity . . . the ensuing  
8 discovery of other models and related products may bring those products within the scope of the  
9 notice.” *Funai Elec. Co. v. Daewoo Elecs. Corp.*, 616 F.3d 1357, 1373 (Fed. Cir. 2010).

10 **a. ’926 Patent**

11 SonicWall believes it is entitled to summary judgment of no pre-suit damages for the ’926  
12 Patent. SonicWall argues that although Finjan alleges it provided SonicWall with actual notice on  
13 June 10, 2014, based on an email from Finjan’s Ivan Chaperot to Dell’s Anthony Peterman, Finjan  
14 did not provide a specific charge of infringement of the ’926 Patent by a specific accused product.  
15 Mot. at 23. Finjan alleges that “licensing discussions between Finjan and Dell, Inc. (SonicWall’s  
16 predecessor-in interest) began in June 2014” and that documents confirm the ’926 Patent was  
17 “among those under discussion.” Opp. at 25 (citing ECF 319-29 at 47998; ECF 319-33 at  
18 146184). It also argues that “SonicWall’s parent company Dell was on notice of the ’926 Patent  
19 from 2014, albeit in a different context.” *Id.* (citing ECF 319-29 at 47993).

20 The Court agrees with SonicWall. The cited evidence is insufficient as a matter of law as it  
21 merely identifies Finjan’s ’926 Patent without reference to a SonicWall product. *See* ECF 319-29  
22 at 47993 (chart mapping the ’926 Patent to RSA Security products), 47998 (chart identifying the  
23 ’926 Patent as a “Finjan Cybersecurity Patent”); ECF 319-33 at 146184 (chart identifying the ’926  
24 Patent as part of “Finjan Inc. US Patent Estate”). “Actual notice requires the affirmative  
25 communication of a specific charge of infringement by a specific accused product or device.”

1 *Amseted*, 24 F. 3d at 187. “General letters referring to the patent and including an admonishment  
2 not to infringe do not constitute actual notice.” *Minks v. Polaris Indus., Inc.*, 546 F.3d 1364, 1376  
3 (Fed. Cir. 2008).

4 **b. ’968, ’780, and ’844 Patents**

5 With respect to the ’968, ’780, and ’844 Patents, SonicWall argues that Finjan has not  
6 established that the products identified pre-suit are “other models” or “related products” to the  
7 now-accused products—and indeed, SonicWall contends that the accused products are  
8 “completely different” from the ones Finjan identified in November 2014. Mot. at 23. According  
9 to SonicWall, the November 2014 presentation “vaguely references various products, but it does  
10 not include a charge of infringement by the products Finjan accuses in this lawsuit.” Mot. at 23  
11 (citing ECF 319-27). Finjan rejects this characterization and points the Court to evidence that  
12 SonicWall was on notice of the ’968, ’780, and ’844 Patents. *See* Opp. at 20-25.

13 The Court agrees with Finjan. There is ample evidence if credited by the jury to support a  
14 finding that Finjan provided appropriate pre-suit notice of the ’968, ’780, and ’844 Patents. *See*  
15 ECF 319-27 at 47895-47903, 47916; ECF 319-28 at 47936, 47938, 47942, 47943; ECF 319-30 at  
16 1044809-1044810; ECF 319-33 at 146174–76. Because there is a genuine dispute of fact on this  
17 issue, summary judgment is improper here.

18 \*\*\*

19 The Court GRANTS SonicWall’s motion for partial summary judgment and finds that  
20 Finjan is not entitled to pre-suit damages for the ’926 Patent. The Court DENIES SonicWall’s  
21 motion for partial summary judgment as to SonicWall’s request for a finding that Finjan is not  
22 entitled to pre-suit damages the ’968 Patent; the ’780 Patent on Finjan’s claims of infringement as  
23 to Capture ATP alone, Capture ATP in combination with Gateways, and Capture ATP in  
24 combination with ES products; and the ’844 Patent as to Capture ATP alone and in combination  
25

the Gateways prior to June 2016 and Capture ATP in combination with the ES products prior to June 8, 2017.

#### IV. ORDER

For the foregoing reasons, the Court GRANTS partial summary judgment in favor of SonicWall and finds as follows:

- (1) SonicWall does not infringe claim 1 of Patent '154;
- (2) The combination of SonicWall's Email Security products and Capture ATP cannot infringe the asserted claims of Patent '844, '494 and '926;
- (3) SonicWall Gateways do not receive "Downloadables" and therefore cannot infringe the asserted claims 10 and 14 of Patent '494, claims 41 and 43 of Patent '844, and the asserted claim of Patent '780;
- (4) SonicWall does not infringe the asserted claims Patents '305 and '408 based on a combination of separate, remote computers;
- (5) SonicWall does not infringe the asserted claims of Patents '926 and '305;
- (6) Finjan is not entitled to a royalty on SonicWall's Non-U.S. Sales; and
- (7) Finjan is not entitled to pre-suit damages for:
  - a. the '926 Patent;

The Court DENIES partial summary judgment with respect to SonicWall's request for a finding that:

- (1) Finjan is not entitled to pre-suit damages for:
  - a. the '968 Patent;
  - b. the '780 Patent on Finjan's claims of infringement as to Capture ATP, Capture ATP in combination with Gateways, and Capture ATP in combination with ES products; and



c. the '844 Patent as to Capture ATP alone and in combination with the Gateways prior to June 2016 and Capture ATP in combination with the ES products prior to June 8, 2017.

**IT IS SO ORDERED.**

Dated: March 5, 2021

  
BETH LABSON FREEMAN  
United States District Judge